Part I (12%) Terms and Facts

1. Give short definitions for the following information security terms:(2)
    a. Covert channel.
    b. Discretionary access control.
    c. ISAKMP/Oakley.
    d. Multilevel security.
    e. Unconditionally secure.
    f. X.509.
2. Which are the common types of firewalls? (1)

Part II (28%) Communication Security

The Secure Socket Layer (SSL) protocol is now a de facto standard for HTTP transport security. Network level security services are defined in the IETF IPsec architecture and protocol standards.

3. Which processing steps are carried out in the SSL Record Protocol sender operation? (1)
4. Why is there a separate *Change Cipher Spec* protocol in SSL, rather than just including a "change_cipher_spec" message in the Handshake Protocol? (1)
5. What are the principal security services provided by IPsec? (1)
6. What is the difference between transport and tunnel modes in IPsec? (1)
7. Draw a protocol stack diagram that arranges all security protocols presented in this course relative to the TCP and UDP protocols. Use your protocol stack diagram and list the advantages and disadvantages of putting the security services of confidentiality and integrity/authenticity at each of the specific layers. (3)

Part III (28%) Message Security

Individuals and organizations have come to rely heavily on e-mail services, but message security has yet to be adopted on a large scale. The PGP scheme provides a "pretty good" security solution for file handling and e-mail communications.

8. PGP message processing provides five principal services. What are they, and in which sequence are they performed at the sender side? (1)
9. PGP makes use of the cipher feedback (CFB) mode of symmetric block encryption with 64-bits feedback, whereas most symmetric encryption applications use the cipher block chaining (CBC) mode. Electronic Code Book mode (ECB) encryption can be defined as $C_i = E_K(P_i)$, where $E_K()$ is the block cipher, K is the key, P_i is the i'th plaintext block and C_i the corresponding ciphertext block. Give the algebraic definitions for CFB and CBC modes of encryption. (1)
10. With the ECB mode, if a channel error occurs in a block of the transmitted ciphertext, only the corresponding plaintext block is affected at the receiver side. However, in the CBC mode, this error will propagate at the receiver side. For example, an error in the transmitted C_1 obviously corrupts both P_1 and P_2. Are any blocks beyond P_2 at the receiver corrupted by this channel error? Explain your answer. (1)

11. With the CBC mode, suppose that there is one bit error in the source version of P_1, that is, prior to sender encryption.
    a) Through how many ciphertext blocks is this *source error* propagated by the sender encryption? Explain your answer. (1)
    b) Assuming an errorless channel, what is the effect on the plaintext at the receiver after decryption? (1)
12. Recall that the PGP scheme allows a user to operate with multiple public/private key pairs. The leading two octets of the message digest are included in the clear in the signature part of the PGP message. The purpose of this is to help the verifier determine if she is using the correct RSA public key of the sender.
    a) To what extent does this compromise the security of the SHA-1 hash algorithm? (1)
    b) To what extend does it perform its intended function, namely, to help determine if the correct RSA key was used to decrypt the digest? (1)

Part IV (24%) Cryptography

Alice and Bob will communicate over an open channel. But prior to using symmetric key encryption Alice wants to be able to confirm that they are both in possession of the same secret key. Alice suggests the following protocol:
First she will create a random bit string the length of the key, XOR it with the key, and send the result to Bob. Bob will XOR the incoming message with the secret key and return the result to Alice. Then Alice compares the returned result with her original random string. If equal, she is satisfied that Bob possesses the same secret key, yet neither of them has communicated the secret key directly.

13. Explain the security problem of this protocol. (1)
14. Bob suggests fixing the detected flaw in Alice's protocol by using a one-way function. Take on Bob's suggestion and work out a protocol that may be used instead of Alice's flawed proposal. (2)
15. The RSA public key of Bob is (e = 13, n = 253). Explain how you can find his private key, and use your description to compute his private key. (2)
16. You intercept an RSA ciphertext sent to Bob. How can you compute the plaintext? Specifically, what is the plaintext M if the ciphertext C = 2 is intercepted?(1)

Part V (8%) Legal Issues

17. What is the notion of "personal data" according to the Norwegian Personal Data Act? (Hva er en "personopplysning" slik Personoppplysningsloven definerer begrepet?) (1)
18. Present at least two of the conditions required by the Norwegian Personal Data Act for processing of personal data. (Nevn minst to krav som Personopplysningsloven stiller til behandling av personopplysninger.) (1)
